DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
2531 JEFFERSON DAVIS HWY
ARLINGTON VA 22242-5160

IN REPLY REFER TO
5239
SER 00I/P13
15 APR 02

POLICY LETTER 13-02

From: Naval Sea Systems Command, Chief Information Officer (SEA 00I)

Subj: INFORMATION ASSURANCE POLICY FOR NETWORKED MULTI-FUNCTIONAL DEVICES

1. Purpose: The purpose of this document is to define the Information Assurance policy for the use of Multi-Functional Devices (MFDs) within NAVSEA-HQ, as well as defining standard procedures for dealing with security incidents involving these machines.

2. Scope: This policy applies to the NAVSEA Headquarters Campus at the Washington Navy Yard and the NAVSEA Non-Relocating Offices.

3. Discussion:

a. MFDs are machines connected to the Information Technology networks that perform all the functions of printer, copier, scanner, and FAX. Because these devices are controlled and operated by a general-purpose computer, DoD/DoN computer security policies apply. Historically, a separate device performed each of these functions and often the machines were dedicated to individual users. NAVSEA-HQ is now replacing this large collection of diverse machines with a much smaller number of standard MFDs, each of which will be shared by multiple users via the network.

b. Members of the NAVSEA-HQ workforce routinely handle information at all levels of security classification. Therefore, MFDs will be available for use at each classification level. The MFDs have the ability to store and transmit information and, as such, create the possibility of information being processed on machines at inappropriate security levels. If and when a security breach occurs, it must be quickly and effectively corrected.

4. Policy: The following policies will be enforced to assure the proper safeguarding of information processed on the MFDs:

a. A government-recognized certification laboratory is required to validate the security of multiple network connections. Pending validation, only one network connection per MFD will be permitted. This will preclude the use of MFDs as both network printers and FAX machines.

b. All MFDs will be assigned a security classification level that will be indicated by prominent labeling on the machine.

c. MFDs will not be used to process information above the classification level designated.

d. All MFDs will have the Automatic Job Recovery feature disabled where applicable.

e. All MFDs will have the "scanning to e-mail" feature disabled.

f. All MFDs will have software patches applied to harden the systems against known vulnerabilities where applicable.

g. All MFDs shall enable the "automatic banner page" feature as the default for each print job to ensure accountability.

h. All MFDs will use password protection for administrator and maintenance access. All default passwords will be changed immediately upon machine installation.

i. Any storage media removed from an MFD shall remain the property of NAVSEA. NAVSEA will be responsible for the proper disposal of all storage media.

j. Laptops and other devices connected to MFDs by service technicians for maintenance are subject to the same media disposal requirements as the MFD. Any storage media contained in such devices will remain the property of NAVSEA and will not be removed from NAVSEA spaces. NAVSEA will be responsible for the proper disposal of any storage media from these devices.

k. All images scanned by an MFD will go to personal repositories, not public repositories.

l. Additional features will be precluded from enabling until specific needs have been identified and justified.

m. MFDs used for processing classified information shall:

(1) Be afforded the physical security appropriate for the level of information being processed.

(2) Use removable hard drives as appropriate.

(3) Enforce the use of automatic hard disk overwrite software to the maximum extent possible, when available.

5. Individual Responsibilities:

a. The NAVSEA Deputy CIO for Enterprise Information Assurance shall:

(1) Approve, promulgate, and maintain these instructions.

(2) Periodically review the database of past incidents looking for trends and considering needed changes to policies and procedures.

b. The NAVSEA Deputy CIO for IT Operations and assigned Division Personnel shall:

(1) Ensure all MFDs are configured and maintained in accordance with the provisions of this policy.

(2) Ensure all MFDs prominently display a label indicating the level of classification authorized for processing.

(3) Ensure that directions are prominently and clearly posted near each MFD to provide information on the actions to be taken if the MFD was used to process information classified higher than authorized.

(4) Maintain an inventory of all MFDs, including location, security designation, and history of all instances of inappropriate usage. In addition, an inventory of all hard disks in MFDs used for classified processing, including drive serial number and MFD identification code, will be maintained. This inventory will include drives in unclassified machines that are still in use after having been sanitized from inadvertent processing of classified information.

(5) Sanitize or dispose of classified media in accordance with the latest DoD guidance, via the NAVSEA Test and Reutilization Center (TRC).

(6) Take action on user calls regarding the use of MFDs for processing information at a higher level of classification than permitted.

c. Individual MFD users shall:

(1) Use MFDs according to the posted classification markings.

(2) Use user-defined PINs to authorize the release of print jobs.

(3) Users shall retain the "automatic banner page" default for each print job to ensure accountability.

(4) In cases involving unauthorized processing of classified information, immediately perform the following actions:

(a) Immediately power off the MFD, and post a sign on the MFD stating "Down for Security. Do Not Restart."

(b) Notify the NAVSEA Help Desk.

(c) Follow instructions from the Help Desk.

6. Unauthorized Classified Processing: In cases involving unauthorized processing of classified information, the following principles shall be observed:

a. Precedence shall be given to service calls involving inappropriate processing of classified information.

b. Once arriving on the scene of a security breach notification, the Help Desk Technician shall not leave the MFD unattended until the proper hard drive overwrite or removal procedures are completed.

c. As an MFD becomes damaged beyond reasonable repair and is returned to the vendor, the hard drive(s) shall be removed and placed in the custody of the TRC for degaussing and disposal. If after hours, the Help Desk Technician shall deliver the drive(s) to the TRC watch officer for overnight storage.

d. In case of processing unauthorized information on an MFD, the hard drive(s) must be properly sanitized by an overwrite process with the approved functions and capabilities described in Section 2.1, Attachment 2, of the Assistant Secretary of

Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives, dated June 4, 2001. If the overwrite process cannot meet these standards, the hard drive(s) must be removed and placed in the custody of the TRC for degaussing and disposal.

e. Standard procedures shall be executed as approved by the NAVSEA Chief Information Officer.

7. The POC for this policy is the Deputy CIO for Enterprise Information Assurance, Mr. Tony Geddie, (202)781 3014.

S.J. BOURBEAU
CHIEF INFORMATION OFFICER
NAVAL SEA SYSTEMS COMMAND